Amanda R. Grier
Colleen B. Robbins
Elsie B. Kappler
FEDERAL TRADE COMMISSION
(Each appearing pursuant to DUCivR83-1.1(e))
Attorneys for Plaintiff
Division of Marketing Practices
600 Pennsylvania Ave., N.W., CC-8528
Washington, DC 20580
Telephone: (202) 326-3745
agrier@ftc.gov
crobbins@ftc.gov
ekappler@ftc.gov

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH
CENTRAL DIVISION

FEDERAL TRADE COMMISSION,

Plaintiff,

v.

ELITE IT PARTNERS, INC., a Utah corporation doing business as ELITE IT HOME, and

JAMES MICHAEL MARTINOS, individually and as an officer of ELITE IT PARTNERS, INC.,

Defendants.

Case No. 2:19cv125

FILED UNDER SEAL PURSUANT TO COURT ORDER (DOCKET NO. _____).

PLAINTIFF'S MOTION FOR *EX PARTE* TEMPORARY RESTRAINING ORDER WITH ASSET FREEZE AND OTHER EQUITABLE RELIEF AND ORDER TO SHOW CAUSE WHY A PRELIMINARY INJUNCTION SHOULD NOT ISSUE AND MEMORANDUM IN SUPPORT

Table of Contents

Table of Authorities

Cases

Statutes

Rules

Regulations

Table of Exhibits

I. INTRODUCTION AND REQUESTED RELIEF

Plaintiff Federal Trade Commission ("FTC") asks the Court to halt a long-running computer technical support scam and order Defendants to provide redress to the thousands of consumers—primarily older adults—who have been harmed. The scam, operated by Defendants Elite IT Partners, Inc. ("Elite") and James Martinos, utilizes fake computer diagnostics and misleading, false, and unsubstantiated statements that scare consumers into believing that computer viruses have hijacked their computers, exposing their personal and financial information to hackers.[1] Relying on these false statements, thousands of consumers have purchased costly "cleanings" from Elite, and enrolled in long-term maintenance plans. Elite fails to disclose key terms to consumers prior to obtaining payment, including annual automatic renewals and a steep $150 early cancellation fee. When consumers or Elite's employees become wise to the scam, Defendants often intimidate them with persistent threats of litigation and collection actions. Defendants actively conceal the true nature of their scam, deceiving not just consumers, but also Elite's employees, credit card payment processors, banks, and credit card companies. Since 2015, Defendants have taken at least $10.7 million from consumers through their deceptive practices.

Defendants' conduct violates (1) Section 5(a) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45(a), (2) the FTC's Telemarketing Sales Rule ("TSR"), 16 C.F.R. Part 310, as amended, and (3) Section 4 of the Restore Online Shoppers' Confidence Act ("ROSCA"), 15 U.S.C. § 8403.

[1] The FTC submits four volumes of exhibits in support of its motion. All exhibits cited in this Memorandum are referenced as "PX [exhibit number]." References to declarations include a relevant paragraph number, and attachments are designated with a relevant page number. In considering an application for a TRO or preliminary injunction, the Court "may rely on affidavits and hearsay materials" if appropriate. *Levi Strauss & Co. v. Sunrise Int'l Trading, Inc.*, 51 F.3d 982, 985 (11th Cir. 1995).

REQUESTED RELIEF: Plaintiff FTC respectfully moves the Court *ex parte* for a Temporary Restraining Order ("TRO") that will protect consumers, prevent further harm, and preserve the Court's ability to provide complete and permanent relief to the injured. The FTC has proposed a TRO that will immediately halt Defendants' scam, freeze Defendants' assets, appoint a temporary receiver, and provide immediate access to Defendants' business premises in order to preserve assets and documents for consumer redress. The FTC also requests that the Court order Defendants to show cause why a preliminary injunction should not issue against them. The Proposed TRO is attached.

II. STATEMENT OF FACTS

A. Defendants Operate a Computer Technical Support Scam.

Since at least 2013, Defendants have employed a bait-and-switch deception, which primarily affects older adults.[2] They lure consumers to provide their contact information with the promise of recovering a forgotten email password, account login, or other one-time technical support problem, but actually deliver fake diagnostics and false statements designed to deceive consumers into purchasing unnecessary technical support services.

[2] Elite's former employees report that its customers were primarily older adults. *See, e.g.*, PX 15 at 120 (former Elite employee stating that customers were "mostly elderly individuals"); *Id.* at 122 (another former employee stating that "customers were primarily elderly and could not understand what was being said"); *Id.* at 130 (a third former employee recalling: "the customers were entirely elderly who 'didn't know anything'"); *Id.* at 130 (a fourth former employee stating: "most of the customers he spoke to as a [customer service representative] were elderly, maybe 60-70 years old or older. Many of them were confused about the charges they had on their credit card, or were people calling in about charges on their elderly parents' cards and were trying to cancel. These were the majority of the calls that [he] received as a [customer service representative]"); PX 13 ¶18 ("Almost all of the customers I spoke with were elderly. I knew these customers were elderly by the sound of their voices, and the fact that many referred to grown children and grandchildren. In addition, in my conversations with other employees, including salespeople, we frequently discussed the fact that vast majority of Elite IT's customers were elderly."); PX 20, p. 975 ("The majority of the customers I dealt with were elderly."). Consumers also complain that Elite is targeting older consumers. *See, e.g.*, PX 27 ¶ 4-5 ("30 consumers identified Elite as profiling elderly individuals.").

The Commission has confirmed Defendants' deceptive actions through various means. FTC staff spoke with numerous consumers who filed complaints with the FTC, Better Business Bureau ("BBB") and Utah's Division of Consumer Protection ("DCP").[3] Commission staff also interviewed former Elite employees who stated that the telemarketers are trained, among other things, to (1) make false statements to consumers about the presence of viruses on consumers' computers through a three-part diagnostic test,[4] (2) falsely tell consumers Elite provides support for Yahoo and AOL,[5] and (3) use scare tactics to make sales.[6]

FTC staff also conducted several undercover calls confirming both consumers' testimony and the former employees' accounts.[7] A computer expert analyzed these calls and detailed Elite's deception in his report.[8] Microsoft's Digital Crimes Unit, independent of the FTC's investigation, also conducted an undercover purchase.[9] Through the undercover calls, staff confirmed that Defendants only provide their sale terms and conditions *after* consumers make their payment, including a $150 early cancellation fee and a negative option for a long-term maintenance package.[10] The long-term maintenance plan option is in fact a 12-month plan with automatic renewal.[11] Accordingly, as discussed more fully below, Defendants' practices are deceptive and violate the FTC Act, 15 U.S.C. § 45(a), the TSR, 16 C.F.R. § 310.3(a)(4) and (a)(1), and ROSCA, 15 U.S.C. § 8401.

---

[3] *See, e.g.*, PX 1; PX 2; PX 3; PX 4; PX 5; PX 6; PX 7; PX 8; PX 9; PX 10; PX 11; PX 12.
[4] PX 15, pp. 120, 122, 129, 131.
[5] PX 13 ¶ 20; PX 15, pp. 120-124, 127-128, 131.
[6] PX 20 ¶ 21.
[7] PX 18 ¶¶ 4-65; PX 17 ¶¶ 4-50; PX 28 ¶¶ 10-45.
[8] PX 14 (expert report).
[9] PX 16 ¶ 3.
[10] PX 14, pp. 220-23; PX 15, p. 120, PX 17, pp. 218-223; PX 18 ¶ 38-39; PX 28 ¶¶ 22, 41.
[11] PX 17, pp. 218-223; PX 28 ¶¶ 22, 41.

1. Defendants Use Deceptive Tactics to Remotely Access Consumers' Computers.

a. Initial Contact—Online Search Advertisements

Often, the deception begins with Elite's advertising. Elite purchases keyword advertisements from search engine platforms, such as Google Adwords.[12] To advertise with keywords, an advertiser pays to have an advertisement appear in the results listing when a person uses a particular phrase to search the Web. When a person uses the purchased keywords in a Google search, Elite's ads display prominently as a paid search result.[13] For example, Elite specifically targets persons who have forgotten their email passwords with the search terms "forgot my email password."[14] Elite also purchased search terms related to "Yahoo, AOL, and Verizon support," targeting consumers seeking technical support from a specific company.[15]

When a user enters "forgot my email password," as FTC investigators did, Elite's ads display prominently as a search result.[16] After clicking on the advertised search result, consumers are automatically re-directed to one of Elite's webpages offering a "Free, No Obligation PC diagnostic" that states "EMAIL PROBLEMS? SPEAK TO LIVE AGENT for free!"[17] The webpages request the consumer's name, email, and telephone number to "help diagnose your problem with one of our Elite IT™ Techs."[18] An Elite sales representative then calls the number provided by the consumer.[19]

---

[12] PX 19, pp. 848-49; PX 15, p. 121; PX 17 ¶¶ 18-25; PX 18 ¶¶ 11-14; PX 28 ¶¶ 11-13.
[13] *Id*.
[14] PX 17 ¶¶ 18-26; PX 18 ¶¶ 11-15; PX 28 ¶¶ 11-14.
[15] PX 15, p. 151.
[16] PX 17 ¶¶ 18-26; PX 18 ¶¶ 11-15; PX 28 ¶¶ 11-14.
[17] *Id*.
[18] *Id*.
[19] *Id*.

b. Initial Contact—Cold Calls

Elite also cold calls consumers. Many consumers are surprised to receive a phone call regarding their computer, and do not know how Elite obtained their contact information.[20] Consumers that have received these calls have no memory of filling out the online form described above.[21] Former employees confirmed that Elite made outbound calls to consumers, and noted that many consumers were surprised by the call.[22] Many consumers believed that Elite's telemarketers worked for their email provider or some other well-known company.[23] According to former employees, Elite instructed its employees to explicitly tell or implicitly suggest to consumers that Elite provides support for, or partners with, Yahoo and AOL, or Verizon.[24]

c. The Sales Pitch

Whether the initial contact is through an online search advertisement or a cold call, once Elite has a consumer on the phone, Elite directs its employees to gain remote access to the consumer's computer and pitch their technical support "cleanings" and maintenance.[25] Remote access gives Elite's telemarketers control over the computer—the telemarketer can move cursers, enter commands, run applications, and access stored information. Elite trains its employees to obtain remote access to the consumer's computer to run diagnostics—regardless of the stated problem.[26] Even when consumers report that they have simply forgotten their email password, Elite instructs its employees to explain that a virus is likely blocking the consumers' email

[20] *See, e.g.*, PX 3 ¶ 5; PX 5 ¶ 3; PX 6 ¶ 2.
[21] *Id*.
[22] PX 13, ¶ 15; PX 15, p. 128.
[23] PX 3 ¶ 5; PX 12 ¶ 3; PX 13 ¶ 20; PX 15, pp. 120, 131.
[24] PX 13 ¶ 20; PX 15, pp. 120-124, 127-128, 131.
[25] PX 15, p. 124; PX 20 ¶ 8.
[26] PX 20 ¶ 8.

access, and Elite must remotely access their computers to diagnose and fix the problem.[27] According to a former employee, "[s]ometimes customers were not locked out of their email; they just did not know how to enter their user name and password to log in."[28] Elite's telemarketers promise that Elite's technicians will be able to recover email passwords, even though Elite's terms of service stated that email recovery is not guaranteed.[29] A customer service representative fielding complaints stated that "[a]pproximately 80% were upset that Elite IT had not yet helped them access their email as promised."[30]

During four undercover calls, FTC investigators found Elite's advertisements by searching "forgot email password" and told Elite's staff that they had forgotten their email password. Each time, Elite's staff insisted that they must remotely connect to the computer and run a diagnostic first despite the fact that email providers often offer free and simple recovery services for forgotten passwords.[31]

2. Defendants Misrepresent Their Diagnostic to Scare Consumers into Immediately Purchasing Expensive and Unnecessary "Cleanings."

While in control of a consumer's computer, Elite sales representatives run a diagnostic that it falsely claims will make sure there are no infections or other issues causing problems on the consumer's computer.[32] This diagnostic includes: (1) running a free version of a program named SuperAntiSpyware and misstating the results, (2) opening Windows Task Manager and

---

[27] *See, e.g.*, PX 15, p. 120 (a former employee recalling that Elite managers instructed employees to tell consumers who called for support accessing their Yahoo accounts that "you probably put in your password right, but the viruses are preventing you from signing in."); *Id*. at 124 (former employee did not believe that viruses were the reason for being locked out of their emails but believed that most of these users simply forgot their passwords); PX 17 ¶ 35; PX 18, pp, 292-293; PX 28, pp. 1062-1063, 1067, 1113-1114, 1117.
[28] PX 13 ¶ 19.
[29] PX 15, p. 131.
[30] PX 13 ¶ 24.
[31] PX 15 ¶ 12; PX 17, pp. 184-186; PX 18, pp. 277-278; PX 28, pp. 1055-1056, 1106-1107.
[32] PX 17 ¶¶ 29-32; PX 18 ¶¶ 16-24, pp. 474-475, 493; PX 28 ¶ 32, and pp. 502, 538.

misstating its function and content, and (3) checking for pre-existing antivirus software in the wrong place (and ignoring obvious signs of a functioning antivirus software).[33] This process is not a diagnostic test designed to identify the source of computer problems. Rather, it is part of a scripted sales pitch that inevitably leads to the conclusion that consumers' computers are severely compromised and in need of immediate repair by Elite's technicians.[34]

a. SuperAntiSpyware

Often, Elite telemarketers begin their purported diagnostic by installing and running a free version of the software program, "SuperAntiSpyware," on the consumer's computer.[35] The program inevitably identifies tracking cookies as "Detected Threats" highlighted in red with a red siren symbol.[36] As one former employee put it: SuperAntiSpyware would "find a speck of dust on the computer and deem it a virus."[37]

Elite tells the consumer that these "threats" and tracking cookies are infections on the computer and must be removed immediately to prevent a security breach.[38] In one undercover call, the Elite telemarketer said that SuperAntiSpyware found infections indicative of keystroke

[33] PX 17 ¶¶ 33-36; PX 18 ¶¶ 25-33; PX 20, ¶¶ 8-9; PX 28 ¶¶ 17-20, 34-38.
[34] PX 13 ¶ 9 (former employee stated, "sales representatives were supposed to explain to consumers that the performed diagnostics revealed that their computers were likely infected with viruses, and that their personal information was at risk if they did not take immediate action"); PX 20 ¶¶ 8-10 (Elite's former employees recalled that "I could always find one or two things to point out to the consumer").
[35] PX 15, p. 127; PX 17 ¶¶ 33-34; PX 18 ¶ 27; PX 20 ¶ PX 28 ¶¶ 17, 34.
[36] PX 14, p. 90; PX 17 ¶ 34; PX 18, pp. 337-38; PX 28 ¶¶ 18, 35; *See also,* PX 15, p. 122 (a former customer service manager recalled that "sales staff conducted scans of customer computers and claimed that cookies were viruses which 'could wipe out the computer'").
[37] PX 15, p. 131. Some Elite telemarketers noticed that the same free version was available online, and ran the program on their own computers (sometimes with the know-how of a more tech savvy person). Invariably, the program also found "threats" and "tracking cookies" on their computers, which they noted was removed with the click of a button. PX 15, p. 128.
[38] PX 17 ¶¶ 34-38; PX 18, pp. 288-294; PX 28, pp. 1062-1063, 1066-1067, 1113-1119.

loggers that steal data on a computer.[39] These statements are false. According to the FTC's expert, Harold Pomeranz,[40] the program did not find a keystroke logger; rather, it found innocuous tracking cookies.[41] Tracking cookies are not keystroke loggers, "infections," or malicious programs, cannot steal data from a computer system, and are no threat to the security of the system.[42]

b. Windows Task Manager

In another step of the deceptive "diagnostic" test, Elite telemarketers open the Windows "Task Manager" on the computer and falsely state that the CPU percentage and number of processes running are too high, claiming these are "red flags" and indicators that the computer has been working too hard.[43] This is false. Not only are computers designed to run at maximum power for long periods of time, but CPU percentage and the number of processes on the system are not "red flags" or indicative of the presence of infections, as suggested by the representatives.[44] According to the FTC's expert, "this claim is nonsense."[45]

c. Msconfig Start-Up Tab

To further convince consumers that their computers are infected, Elite employees open the "msconfig" start-up tab, and claim that it shows that no antivirus program is running on the

[39] PX 17 ¶¶ 33-35.
[40] Harold Pomeranz is the founder and technical lead of Deer Run Associates, a consulting company focusing on computer forensic investigations and information security. Mr. Pomeranz has more than twenty-five years of experience working with computer and information security issues for global commercial, government, and academic organizations. He is also an Instructor and Faculty Fellow of the SANS Institute, the global leader in technical information security training.
[41] PX 14, pp. 73-74.
[42] *Id*.
[43] PX 14, pp. 74, 79; PX 28, pp. 1118-1119.
[44] PX 14, pp. 74, 79.
[45] *Id*.

computer.[46] The employee falsely states that a functioning antivirus program should appear in the msconfig start-up tab, because, as the telemarketer explains, an antivirus program should be the first program to run before anything else.[47] According to an Elite telemarketer, the absence of an antivirus program name in this tab proves that an antivirus program is non-existent or not functioning properly.[48] In truth, the msconfig start-up tab does not determine the existence of an antivirus program, as antivirus programs often start after the Windows operating system has begun.[49] Moreover, Elite employees ignore the presence of existing antivirus programs identified in the msconfig start-up tab. During the FTC's undercover calls to Elite, employees ignored the fact that the computer's antivirus program, "Microsoft Security Client," was explicitly named in the tab. Contrary to the false statements made by Elite, Microsoft's antivirus and security software was installed and running on the systems at the time of the calls.[50]

3. Defendants Misrepresent Their Affiliation with Well-Known Companies.

Elite telemarketers lead consumers to believe they are affiliated with well-known tech companies like Yahoo, AOL, Microsoft, and Verizon, and have even explicitly and falsely claimed that certain companies do not provide technical support or no longer exist.[51] Like the email password deception, Elite purchased online search terms related to "Yahoo, AOL, and

[46] PX 14, pp. 75, 84; PX 28, p. 1066.
[47] PX 14, pp. 75, 84.
[48] PX 28, p. 1066.
[49] PX 14, pp. 75, 84.
[50] PX 14, pp. 75, 84; PX 22 ¶ 6.
[51] PX 13 ¶ 20; PX 15, pp. 120-124, 127-128, 131; *see also* PX 15 ¶ 11 (Elite IT is not affiliated with Yahoo or AOL, and Yahoo and AOL continue to exist and provide support for its tech services, including free email recovery services); PX 26 ¶ 4 (Elite IT is not authorized to perform customer support services on behalf of Microsoft).

Verizon support," thereby targeting consumers searching for tech support from a specific named company.[52]

According to a former Elite Customer Service Manager, Elite's sales scripts instruct staff to "be vague" when asked if they worked for companies like AOL or Verizon.[53] If pressed about the telemarketer's relationship with well-known companies, Elite instructs its telemarketers to say that they "work alongside them" or that they "partnered with them."[54] The same manager recalled listening to calls in which Elite telemarketers told customers that they worked for companies like AOL, Yahoo, or Verizon. When she confronted Elite management about these misrepresentations, Elite management did nothing and the practice continued.[55] In fact, multiple former Elite staff report that Elite "reps outright lied in saying they worked for companies" such as Yahoo, and Elite did nothing to stop it,[56] and that Elite trains its telemarketers to say "[d]id you know that Yahoo and AOL don't exist anymore? They no longer offer technical support so we provide their support" or that "Yahoo had gone under."[57]

Another employee recalled that, during training, an Elite employee instructed him to tell consumers that companies such as Yahoo and AOL do not offer technical support, or charge for such support. When the employee asked the trainer what he should say when a consumer asked for help with a service, like Netflix—which has support—the trainer told him to "make the sale" and lie.[58] A customer service representative (who took calls after a telemarketer had closed the

[52] PX 15, p. 121.
[53] PX 15, pp. 121-23.
[54] PX 15, pp. 121-22.
[55] PX 15, p. 122.
[56] PX 15, p. 123; *see also* PX 15, p. 131 (a former employee recalled that "the Sales staff sometimes lied to customers and told them that they worked for those companies, or didn't make it clear that they did not").
[57] PX 15, p. 120.
[58] PX 15, p. 127.

sale) recalled: "Many of the customers who were transferred to me by sales staff appeared to be under the impression that they were communicating with Yahoo, AOL, or another well-known company.[59] We were never instructed to correct customers' mistaken impression."[60] Consumer complaints corroborate this fact and show consumers believed they were speaking with well-known technology companies.[61]

4. Defendants Use Scare Tactics to Finalize the Sale.

Having convinced consumers that their computers have infections, red flags, or problems, Elite's telemarketers are trained to use scare tactics to convince consumers to immediately purchase a costly "cleaning" from Elite that will remove the purported viruses.[62] Elite's telemarketers ask questions like "do you bank online?" When consumers respond affirmatively, the telemarketer explains that their financial information is at risk.[63] While ignoring the presence of existing functioning antivirus programs, Elite telemarketers tell consumers that their personal and financial information is exposed to hackers and identity thieves whose "goal is to get to email so that they can piece together a lot of information that creates an identity."[64] For example, an Elite telemarketer falsely told an FTC investigator that her passwords were being recorded by keystroke loggers.[65] Employees are trained to tell consumers that "your computer can become susceptible to viruses that can cause you to lose passwords and receive more spam."[66] To consumers who needed help recovering forgotten email passwords, Elite's telemarketers falsely

[59] PX 13 ¶ 20; *see also* PX 27 ¶ 5.
[60] PX 13 ¶ 20.
[61] PX 27 ¶ 5.
[62] PX 13 ¶¶ 9, 33.
[63] PX 17, p. 200; PX 20 ¶ 21.
[64] PX 17, p. 202.
[65] PX 17 ¶ 35.
[66] PX 20 ¶ 21.

state that the "cleaning" will give them email access and solve their problem.[67] The one-time cleaning typically costs $99.99 or more.[68]

5. Defendants Upsell Recurring Service Plans to Consumers.

Using the same misrepresentations and scare tactics, Defendants upsell consumers additional technical support service plans that typically cost $19.99 (Gold Care), $29.99 (Platinum Care), and $39.99 (Unlimited Care) per month.[69] Distinct from the one-time services provided by Elite, these plans also include what Defendants describe as "preventative care" services at increasing levels of frequency (Gold—every 90 days; Platinum—every 45 days; and Unlimited—unlimited technical support during business hours).[70] The service packages automatically renew after twelve months, unless the consumer cancels.[71] Elite charges a $150 cancellation fee if consumers cancel before the end of the twelve-month period.[72] After Defendants enrolled consumers in technical support service plans, they further upsell their upgraded service plans.[73]

6. Defendants Do Not Adequately Disclose Material Terms and Conditions Before Consumers Purchase Their Services.

Once a consumer agrees to pay Elite for its tech support services, the telemarketer requests payment. Elite typically collects payment in one of two ways: (a) by providing an online form for the consumer to directly type payment information, or (b) by verbally requesting

[67] PX 17, pp. 202, 206; PX 18, p. 293; PX 28, pp. 1064, 1067, 1074, 1124.
[68] PX 17 ¶ 40; PX 18 ¶¶ 35-37, and pp. 484, 515-516; PX 28 ¶ 39.
[69] PX 15, p. 130.
[70] *Id*.
[71] *See, e.g.*, PX 18, p. 389.
[72] PX 1 ¶ 5, PX 6 ¶ 10, PX 7 ¶ 12, PX 9 ¶ 3, PX 10 ¶ 4, PX 11 ¶ 5, PX 15, p. 122.
[73] PX 13 ¶ 21.

payment information from the consumer and entering the payment information for the consumer.[74]

Elite does not provide its terms and conditions to consumers prior to payment. If the terms and conditions are given to a consumer at all, it is only ***after*** consumers provide their payment information and the payment is processed.[75] Even then, Elite staff provide it verbally and often fail to read all material terms to the consumer.[76] The terms and conditions are not provided to the consumer on the computer screen, even though the payment form appears to contain a hyperlink to "Terms and Conditions."[77] The consumer is not directed to view the terms and conditions before proceeding with the transaction, and Elite's employee retains control of the computer and its curser by virtue of the remote computer connection.[78] Undercover FTC investigators were told verbally, after payment, that (1) the investigator had authorized the transaction, (2) this is a 12-month plan with automatic renewal, (3) there are no refunds, and (4) the plan can be cancelled at one year.[79] Conspicuously absent from the recital of terms and conditions is the cancellation process and the $150 early cancellation fee.[80]

---

[74] PX 17 ¶ 40; PX 18, p. 351; PX 28, pp. 1077-78, 1126.
[75] PX 15, p. 120, PX 17, pp. 218-223; PX 28 ¶¶ 22, 41.
[76] *See e.g.*, PX 28, pp. 1077-78, 1126.
[77] PX 17 ¶ 40; PX 18, p. 351. According to former employees, they were trained only to read the terms and conditions after they received the payment. *See, e.g.*, PX 20, p. 973 ("I was trained to only read the terms and conditions after I got the payment.").
[78] PX 17, pp. 215-220; PX 18, pp. 296-300. Despite this reality, Defendants routinely falsely claimed to their payment processor in the chargeback process that consumers were told of the terms and conditions prior to payment. PX 28, pp. 1182, 1188, 1194, 1200, 1205, 1211, 1218.
[79] PX 15, p. 120, PX 17, pp. 218-223; PX 28 ¶¶ 22, 41.
[80] *Id*. An email is sometimes sent **post-sale** to the consumer outlining Elite's terms and conditions, including its cancellation process. At the bottom of the email, Elite details some of its terms and conditions, including that (1) there is a $150 cancellation fee if a consumer cancels before the end of the one-year contract, (2) in order to cancel, a consumer must do so in a written letter, 30 days prior to the end of the term, and (3) the support plan will automatically renew for another year at the end of the 12 month period. *See, e.g.*, PX 17, p. 249. However, consumers who have forgotten their password for their email account, the reason for many of the

7. Defendants Employ Threats and Scare Tactics When Consumers or Employees Uncover the Fraud.

Many consumers who complain to Elite find themselves facing collection actions, threats, and intimidation.[81] One former employee explained that the managers expected customer service representatives to threaten legal action when customers disputed their bills.[82] In one such instance, a consumer stated that after she disputed the charges with her credit card company, she received harassing phone calls from Elite for several weeks demanding full payment of nearly $500 and threats to sue her to "make things difficult."[83] Another consumer reported that Elite threatened to refer the matter to collections after she tried to cancel within twelve hours of signing up for the service.[84]

Elite also aggressively and dishonestly disputes consumers' claims that its credit card charges were unauthorized—frustrating consumers' ability to obtain redress while simultaneously legitimizing Elite's threats of litigation and collection actions.[85] When disputing credit card chargebacks from consumers, Elite typically claims that it shows consumers its terms and conditions on the computer and reads them aloud prior to payment.[86] As discussed above, former employees, consumers, and purchases made by FTC undercover investigators confirm that consumers are not informed of the terms and conditions before the payment is processed, and Elite's telemarketers are explicitly told to state the terms and conditions only after payment

---

consumers' calls in the first place, cannot access their email account to receive the email and view the terms and conditions.

[81] PX 3 ¶ 14; PX 6 ¶ ¶ 12, 17; PX 9 ¶ 5; PX 10 ¶ 4.
[82] PX 13 ¶¶ 26-27.
[83] PX 3 ¶ 14-20.
[84] PX 10 ¶ 3.
[85] PX 3 ¶¶ 14, 18-19; PX 28, pp. 1182, 1188, 1194, 1200, 1205, 1211, 1218.
[86] PX 28, pp. 1182, 1188, 1194, 1200, 1205, 1211, 1218.

is received.[87] In some cases, Elite provides no information about the terms and conditions to consumers, either on the screen or verbally.[88]

For example, Elite, while responding to a consumer's credit card chargeback requests, falsely told its payment processor: "On that day, she agreed to Elite IT's Terms of Service and Conditions ("Terms"). Her acceptance of the Terms was required before the agent could proceed with processing her payment."[89] Similarly, in applying to a new payment processor, Elite stated in its merchant application to the acquiring bank that the "[c]ancellation policy is shown to the customer via the Terms section of the billing page and is read to the customer before the sale is complete." James Martinos signed this application, dated August 3, 2018.[90] However, the week prior, an FTC investigator posed as a consumer and Elite's telemarketer did not show the undercover investigator the terms section of the billing page, or read aloud the entire terms and conditions prior to completing payment.[91] The Elite telemarketer also failed to disclose the cancellation fee.[92] Elite failed to show, or otherwise disclose, the material terms prior to purchase every time an undercover investigator made a purchase, including during the most recent purchase on February 5, 2019.[93]

Finally, Elite sued a former employee who posted an online complaint exposing Elite's scam.[94] During settlement discussions, the former employee offered to remove the online

[87] *See supra* notes 77, 79.
[88] PX 13 ¶ 22.
[89] PX 28, p. 1188.
[90] PX 28, p. 1226.
[91] PX 28, pp. 1126-1130.
[92] *Id*.
[93] PX 15, p. 120, PX 17, pp. 218-223; PX 28 ¶¶ 22, 41.
[94] PX 15, pp. 123, 131.

reviews, but Elite demanded more—conditioning settlement on a signed affidavit denying the truth of the review.[95] The former employee declined, refusing to sign a false affidavit.

8. Defendants Openly Defy Utah's Telemarketing Rules, Despite an Administrative Order.

In February 2015, the Utah Division of Consumer Protection ("DCP") sent a formal demand letter to Defendants to file a telemarketer registration with the DCP. Defendants disputed that they are telemarketers and refused to register.[96] In July 2017, the DCP filed a formal Administrative Citation against Defendants for violating the registration requirement.[97] In November 2017, after a two-day hearing and testimony from Martinos, the DCP filed a formal Order of Adjudication against Defendants for violating the registration requirement. This Order required Defendants to cease and desist conducting its business practices without registering as a telemarketer, and imposed a $5,000 fine.[98] Defendants exhausted the administrative process on September 28, 2018, and were denied a stay of the registration requirement throughout this process.[99] Under the terms of the Final Order, Defendants are required to register as a telemarketer and pay fines. They have not, however, registered, paid the fines, or ceased telemarketing.[100] The Utah Attorney General's office filed a Complaint against Defendants on December 3, 2018 for civil enforcement of DCP's Final Order.[101]

9. Defendants Refuse to Stop Deceiving Consumers.

In October 2017, Yahoo's parent company, Oath, sent a letter to Elite demanding that it cease and desist: (1) unfairly charging Yahoo customers significant sums of money for services

---

[95] *Id*.
[96] PX 19 ¶¶ 3, 21-22, p. 586.
[97] PX 19 ¶ 9, p. 630.
[98] PX 19 ¶ 12, p. 940.
[99] PX 19 ¶ 14, p. 943.
[100] PX 19 ¶¶ 21-22.
[101] PX 19 ¶ 22.

Yahoo provides for free; (2) fraudulently misrepresenting themselves as Yahoo employees or authorized representatives of Yahoo; and (3) falsely holding itself out to consumers as Yahoo-certified or sanctioned. Defendants refused to change their business practices. [102]

Recently, in November 2018, Microsoft notified Elite that Elite had been terminated from Microsoft's Partner Network for "fraudulent activity" after an investigation by Microsoft's Digital Crimes Unit.[103] Microsoft found that Elite made false and unsubstantiated statements to Microsoft's undercover investigator when the investigator made a tech support purchase from Elite.[104] Nevertheless, Elite continued to engage in the same deceptive practices, as evidenced by an undercover purchase by an FTC investigator on February 5, 2019.[105]

10. Defendants Knowingly Sought To Deceive Acquiring Banks Regarding the Nature of Elite's Business.

Defendants attempted to conceal and misrepresent the true nature of their business in order to avoid the scrutiny that acquiring banks give to tech support companies. To receive consumer payments via credit cards, Elite (like all merchants) must establish a merchant account at an acquiring bank. Merchants typically create these accounts through payment processors. In so doing, a merchant must properly categorize the nature of its business using a Merchant Category Code ("MCC"). Acquiring banks for credit cards use MCCs to classify a business by the types of goods or services it provides, allowing banks to scrutinize or impose certain restrictions on merchants in higher risk industries, like tech support. Miscoding the MCC is one way that merchants engaging in high risk or illegal activity try to subvert the compliance

[102] PX 15 ¶10, pp. 133-36.
[103] PX 23 ¶¶ 6-7.
[104] PX 16; PX 23 ¶¶ 6-7.
[105] PX 28 ¶¶ 27-43.

mechanisms of acquiring banks—mechanisms designed to detect and prevent illegal or untenably high-risk transactions.

In July 2018, Defendants' then-payment processor, ProPay, notified Defendants that it would no longer process Elite's payments due to excessive credit card chargebacks from consumers.[106] In response, Defendants wrote to ProPay asking that it re-categorize Elite's MCC and create a new merchant account for Elite "to avoid this potential issue with another card processor."[107] In an email, Martinos wrote: "you mentioned Wells Fargo has identified a specific industry that it does not want to service. Can you provide us with the MCC code(s) so we don't repeat this situation…could we just change our category and prevent the closing of our account with ProPay? Or could we open a new account under ProPay with a different category code that would satisfy Wells Fargo's industry concern?"[108] ProPay declined Elite's request and refused to continue processing payments for Elite.[109] After ProPay refused to change Elite' MCC and process its payments, Defendants searched for, and found, a new payment processor.[110]

In Elite's application to a new acquiring bank, Defendants changed Elite's MCC category to "Computers and Computer Peripheral Equipment and Software" and revised Elite's description of its business model as "business to business or wholesale distributors of computer hardware, software and related equipment."[111] In fact, approximately 93% of Elite's business comes from computer repair services to consumers, properly coded as Elite's original MCC with ProPay: "Computer Maintenance, Repair and Services."[112]

---

[106] PX 28, p. 1161.
[107] PX 28, p. 1176.
[108] *Id*.
[109] PX 28, p. 1175.
[110] *Id*.
[111] PX 28, p. 1224 (see MCC code description at PX 28, p. 1177).
[112] PX 24 ¶¶ 12, 14, PX 25 ¶¶ 5-10

B. The Role of the Defendants.

1. Elite Corporate Defendant

Elite is a Utah limited liability company with its principal place of business in Orem, Utah.[113] The company was formed in 2011, and employs sales agents, customer service agents, and computer technicians to sell remote technical support services to consumers throughout the United States and Canada.[114] Elite also claims to have a marketing and business-to-business presence, but, according to bank records, their sales to consumers make up approximately 92% of its revenues.[115] As discussed later, the proposed temporary relief is designed so as not to impact Elite's limited business-to-business component.

2. James Michael Martinos.

James Michael Martinos ("Martinos") is the co-founder of Elite and its CEO.[116] He is actively involved in the operation of this business. For example, Martinos is the signatory on Elite's Wells Fargo corporate account and he lists himself as CEO.[117] He also lists himself as President and CEO of Elite on the merchant services application for ProPay—a payment processor used by Elite until ProPay shut down the account for excessive chargebacks.[118] Martinos opened a merchant account with Complete Merchant Services in September 2018 and migrated Elite's business to this payment processor.[119] Martinos used his credit card to pay for domains, including www.eliteithome.com, and a domain privacy protection service to shield the

[113] PX 18, p. 451.
[114] PX 13, ¶ 12; PX 15, p. 120; PX 18, p. 451.
[115] PX 24 ¶ 12, 14; PX 25 ¶¶ 5-10.
[116] PX 18, p. 451; PX 28, p. 1153.
[117] PX 18 ¶ 68.
[118] PX 28, pp. 1153, 1161.
[119] PX 28, p. 1125.

registration and contact information from the public.[120] Over the course of several years, Martinos reviewed and responded to consumer complaints forwarded to him by Utah's Division of Consumer Protection, and received chargeback notifications from Propay.[121] In September 2017, Martinos testified at a hearing on behalf of Elite after the DCP filed a formal Administrative Citation against Elite for not registering as a telemarketer.[122]

C. Defendants Took At Least $10.7 Million From Consumers Since May 2015.

From May 2015 through August 2018, Elite received over $10.7 million from consumers (minus chargebacks and refunds).[123] The total consumer injury is likely much greater since Defendants opened their merchant processing account in August 2011.[124] According to a former customer service manager, Elite took approximately 250-300 calls per day, and had approximately 4,200 to 4,500 active customers near the end of 2016.[125]

III. LEGAL ARGUMENT

The FTC seeks an *ex parte* TRO halting Defendants' ongoing violations of the FTC Act, the TSR and ROSCA. The FTC requests that the Court enjoin Defendants from these ongoing violations, freeze Defendants' assets to preserve them for restitution to victims, appoint a temporary receiver over Elite, allow the FTC immediate access to Elite's business premises and permit limited expedited discovery. As set forth below, and supported by the FTC's exhibits, the evidence overwhelmingly supports entry of the proposed TRO.

---

[120] PX 18 ¶¶ 83-86.
[121] PX 19, pp. 613-16; PX 28, pp. 1165-70 (chargebacks).
[122] PX 19, pp. 843-79.
[123] PX 24 ¶ 14. One former Elite manager stated that Elite brought in $4.3 million in sales in 2015. PX 15, pp. 121-23.
[124] PX 28, p. 1148.
[125] PX 15, pp. 122-123.

A. This Court Has the Authority to Grant the Requested Relief.

The FTC enforces Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair and deceptive acts or practices in or affecting commerce. The FTC also enforces the Telemarketing Sales Rule, 16 C.F.R. Part 310, which prohibits deceptive and abusive telemarketing acts or practices, and Section 4 of the Restore Online Shoppers' Confidence Act ("ROSCA"), 15 U.S.C. § 8403. Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), gives the Court authority to issue permanent injunctive relief to enjoin practices that violate any law enforced by the FTC and to grant "any ancillary relief necessary to accomplish complete justice."[126] This ancillary relief may encompass "the full range of equitable remedies," including a TRO, a preliminary injunction, an asset freeze, and any other measures that the Court deems necessary to protect consumers and preserve the possibility for complete and permanent relief.[127] Indeed, when the public interest is involved, the court's equitable powers "assume an even broader and more flexible character."[128] The District of Utah and other district courts in the Tenth Circuit have granted the type of preliminary relief the FTC seeks here,[129] including issuing TROs *ex parte*.[130]

---

[126] *FTC v. Commerce Planet, Inc.*, 815 F.3d 593, 598 (9th Cir. 2016).
[127] *FTC v. LoanPointe, LLC*, 525 F. App'x 696, 699 (10th Cir. 2013); *FTC v. Freecom Commc'ns, Inc.*, 401 F.3d 1192, 1202 n.6 (10th Cir. 2005); *see also FTC v. Skybiz.com, Inc.*, No. 01-CV-396-K(E), 2001 U.S. Dist. LEXIS 26175, at *23 (N.D. Okla. Aug 31, 2001), *aff'd*, 57 F. App'x 374 (10th Cir. 2003) ("Section 13(b) also empowers this Court to grant…*any measures* that may be needed to make permanent relief possible.") (emphasis added).
[128] *Porter v. Warner Holding Co.*, 328 U.S. 395, 398 (1946)); *accord Skybiz.com*, 2001 U.S. Dist. LEXIS 26175, at *23-24.
[129] *See, e.g.*, *FTC v. Peterson*, No. 4:18-cv-00049-DN (D. Utah July 10, 2018) (unpublished); *FTC v. Your Yellow Book, Inc.*, No. 5:14-cv-00786-D (Doc. 10) (W.D. Okla. July 25, 2014) (unpublished) (*ex parte* TRO with conduct prohibitions, asset freeze, and financial disclosure requirement); *FTC v. Apply Knowledge, LLC*, No. 2:14-cv-00088-DB (Doc. 16) (D. Utah Feb. 11, 2014) (unpublished) (same); *Skybiz.com*, No. 01-CV-396-K(E) (Doc. 12) (N.D. Okla. June 6, 2001) (unpublished) (*ex parte* TRO with conduct prohibitions and asset freeze); *cf. FTC v. Vision Solution Mktg. LLC*, No. 2:18-cv-00356-TC (Doc. 41) (D. Utah May 4, 2018) (unpublished) (stipulated TRO

B. The Evidence Justifies Granting the FTC's Requested TRO.

To obtain a TRO, the FTC must show "(1) a likelihood of success on the merits; and (2) that a balance of the equities weighs in favor of granting the requested relief."[131] Unlike private litigants, "it is not necessary for the FTC to demonstrate irreparable injury."[132] Here, the FTC meets the requirements to obtain a TRO because the evidence demonstrates that Defendants knowingly operate a tech support scam that continues to harm people.

1. The FTC is Likely to Succeed on the Merits.

a. Defendants Violated Section 5 of the FTC Act.

Defendants' false, misleading, and unsubstantiated representations about the security of consumers' computers violate Section 5 of the FTC Act. In order to establish liability under Section 5 of the FTC Act, "the FTC must establish that: (1) there was a representation; (2) the representation was likely to mislead customers acting reasonably under the circumstances; and (3) the representation was material."[133] A representation is material if it involves information that is important to consumers and is "likely to affect a consumer's choice of or conduct regarding

---

with conduct prohibitions, asset freeze, and financial disclosure requirement); *FTC v. LoanPointe, LLC*, No. 2:10-cv-00225-DAK (Doc. 14) (D. Utah Apr. 2, 2010) (unpublished) (stipulated preliminary injunction with conduct prohibitions and financial disclosure requirement).

[130] When it amended the FTC Act in 1994, Congress reemphasized the FTC's authority to seek preliminary injunctive relief *ex parte*: "Section 13 of the FTC Act authorizes the FTC to file suit to enjoin any violation of the FTC [Act]. The FTC can go into court *ex parte* to obtain an order freezing assets, and is also able to obtain consumer redress." S. Rep. No. 130, 103rd Cong., 2d Sess. 15-16, *reprinted in* 1994 U.S.C.C.A.N. 1776, 1790-91.

[131] *FTC v. Your Yellow Book, Inc.*, No. 5:14-cv-00786-D, 2014 U.S. Dist. LEXIS 116524, at *11 (W.D. Okla. Aug. 21, 2014); *see also Skybiz.com*, 2001 U.S. Dist. LEXIS 26175 at *21-22 (citing *FTC v. World Travel Vacation Brokers, Inc.*, 861 F.2d 1020, 1029 (7th Cir. 1988)).

[132] *Skybiz.com*, 2001 U.S. Dist. LEXIS 26175 at *21-22 ("As irreparable harm is presumed in a statutory enforcement action, the district court need only find some chance of probable success on the merits.") (citing *FTC v. World Wide Factors, Ltd.*, 882 F.2d 344, 347 (9th Cir. 1989)).

[133] *FTC v. Tashman*, 318 F.3d 1273, 1277 (11th Cir. 2003)

[the subject of the representation]."[134] Express and deliberate claims are presumed to be material.[135] In demonstrating that a representation is likely to mislead, the FTC does not need to show that a defendant had the intent to deceive; "[i]nstead, the 'cardinal factor' in determining whether an act or practice is deceptive under §5 is the likely effect the promoter's handiwork will have on the mind of the ordinary consumer."[136] Further, "[w]hile proof of actual deception is unnecessary to establish a violation of Section 5, such proof is highly probative to show that a practice is likely to mislead consumers acting reasonably under the circumstances."[137]

As described above, the Defendants misrepresent to consumers that their computers are in need of repair based on a scripted diagnosis designed to come to the same conclusion every time, regardless of the condition of the consumer's computer, thus inducing consumers to purchase costly and unnecessary technical support and security software. In reality, however, many of the purported issues Defendants identify—including every tracking cookie SuperAntispyware flags and CPU usage—have no impact on the security of a computer or the ability to access consumers' emails.[138] In many instances, including during undercover calls, Defendants falsely identified problems on a pristine computer. As discussed above, these representations are false.[139] In fact, the tools used by Elite telemarketers, and the manner in which they were used, make it very unlikely that they could diagnose any actual security issue.[140]

These express misrepresentations are likely to mislead consumers acting reasonably

---

[134] *LoanPointe*, 2011 U.S. Dist. LEXIS 104982 at *13 (citation omitted); *see also FTC v. Cyberspace.com, LLC*, 453 F.3d 1196, 1201 (9th Cir. 2006) ("A misleading impression created by a solicitation is material if it involves information that is important to consumers and, hence, likely to affect their choice of, or conduct regarding, a product.") (internal quotation omitted).
[135] *LoanPointe*, 2011 U.S. Dist. LEXIS 104982 at *10 (citation omitted).
[136] *Freecom*, 401 F.3d at 1202.
[137] *FTC v. E.M.A. Nationwide, Inc.*, 767 F.3d 611, 633 (6th Cir. 2014) (citation omitted).
[138] PX 14, pp. 68-69, 73-74, 76.
[139] PX 14, pp. 73-75, 80-81, 83-84.
[140] PX 14, p. 68.

under the circumstances. Defendants prey upon consumers' lack of technical sophistication and obvious concern about the operation of their computers and security of their personal and financial information. Not only do Defendants falsely claim their computers are in need of repair, but they use a convincing scan that displays non-existent problems to induce consumers to purchase their services. Given this level of trickery and the number of consumers who have purchased their services, the Defendants' claims are likely to mislead reasonable consumers.

Finally, the representations are material. Defendants' claims go the core of consumers' concerns about their computers' security, and are designed to scare them into purchasing unneeded software and repairs. It is difficult to imagine any consumer who would purchase Defendants' products had Defendants been candid about the fact that their telemarketers had no idea whether there was anything wrong with consumers' computers. Defendants' claims are presumed to be material because they are express claims.[141]

Defendants also violated Section 5 of the FTC Act by making false and misleading representations about their affiliation with well-known internet service and email providers when no such affiliation exists. Specifically, Elite telemarketers have told consumers that they are IT support for Yahoo, AOL and Microsoft or that these companies no longer exist or do not provide support.[142] These representations are false.[143] They are also likely to mislead consumers acting reasonably under the circumstances, and are material to consumers' decisions to purchase Defendants' security repairs and software programs.[144]

---

[141] *FTC v. Pantron I Corp.*, 33 F.3d 1088, 1095-96 (9th Cir. 1994 (*en banc*).
[142] PX 13 ¶ 20; PX 15, p. 120-124, 127-128, 131.
[143] PX 15 ¶ 11; PX 26 ¶ 4.
[144] PX 1 ¶ 3; PX 2 ¶ 3; PX 4 ¶ 4; PX 7 ¶¶ 3-4; PX 9 ¶ 2; PX 12 ¶¶ 4-5.

b. Defendants Violated the TSR.

The Telemarketing Sales Rule (16 C.F.R. Part 310) prohibits any seller or telemarketer from making a false or misleading statement to induce any person to pay for goods or services or to induce a charitable contribution. 16 C.F.R. § 310.3(a)(4). Defendants are engaged in "telemarketing," as defined by Section 310.2(gg) of the TSR because they arrange for the sale of goods or services. Defendants violated Section 310.3(a)(4) of the TSR by misrepresenting that numerous innocuous items on consumers' computers constitute evidence of viruses and they are affiliated with well-known technology companies, including Yahoo, AOL, and Microsoft.[145] Defendants also violated the express terms of Section 310.3(a)(1) of the TSR by failing to disclose, clearly and conspicuously and prior to a consumer consenting to pay for goods or services offered, (1) the total costs to purchase, (2) material restrictions, limitations or conditions to purchase, (3) that the seller will not provide a refund, and (4) the material terms of the negative option.[146]

c. Defendants Violated ROSCA.

Section 4 of ROSCA, 15 U.S.C. § 8403, requires that online businesses engaging in negative option marketing: (1) provide text that clearly and conspicuously discloses all material terms of the transaction before obtaining consumers' billing information, (2) obtain consumers' express informed consent before charging for their services, and (3) provide a simple mechanism to stop recurring charges. Elite fails to follow these requirements.[147]

2. The Equities Weigh in Favor of Granting the FTC's Requested Relief.

Not only has the FTC demonstrated a likelihood of success on the merits, but the balance

[145] PX 14, pp. 73-75, 80-81, 83-84; PX 13 ¶ 20; PX 15, p. 120-124, 127-128, 131.
[146] PX 1 ¶ 4; PX 2 ¶ 6; PX 6 ¶ 5; PX 9 ¶ 3; PX 12 ¶ 5; PX 15, p. 120, PX 17, pp. 218-223; PX 28 ¶¶ 22, 41.
[147] PX 15, p. 120, PX 17, pp. 218-223; PX 18, pp. 351, 389; PX 28 ¶¶ 22, 41, pp. 1077-1078.

of the equities also weighs in favor of granting the requested relief. "When a district court balances the hardships of the public interest against a private interest, the public interest should receive greater weight."[148] No individual has a legitimate interest in continuing to operate an unlawful scheme; thus, "there is no oppressive hardship to defendants in requiring them to comply with the FTC Act, refrain from fraudulent representation, or preserve their assets from dissipation or concealment."[149] Where the danger of asset dissipation exists, "the public interest in preserving the illicit proceeds of the [ ] scheme… is great."[150] Indeed, "a court of equity … has no duty...to protect illegitimate profits or advance business which is conducted by [unlawful] business methods."[151]

3. James Michael Martinos is Liable.

To obtain injunctive relief against an individual for a business entity's unlawful activities, the FTC must show that the individual participated directly in the unlawful activities or had the authority to control them.[152] An individual's controlling ownership of a closely held entity creates "a substantial inference" that the individual had the requisite authority to control.[153] Further, "a corporate officer is presumed to be in control of a small, closely held corporation and assuming the duties of a corporate officer is probative of an individual's participation or authority."[154]

---

[148] *Skybiz.com*, 2001 U.S. Dist. LEXIS 26175 at *23 (citing *FTC v. Affordable Media, Inc.*, 179 F.3d 1228, 1236 (9th Cir. 1999)). "Balancing the equities tips in favor of the public interest in issuing such relief to federal agencies like the FTC." *Id*. at *22 (citing *World Wide Factors*, 882 F.2d at 347.
[149] *World Wide Factors*, 882 F.2d at 347.
[150] *Affordable Media*, 179 F.3d at 1236.
[151] *FTC v. Thomsen-King & Co*., 109 F.2d 516, 519 (7th Cir. 1940).
[152] *Freecom*, 401 F.3d at 1202-03; *LoanPointe*, 2011 U.S. Dist. LEXIS 104982 at *25-26.
[153] *Freecom*, 401 F.3d at 1205.
[154] *LoanPointe*, 2011 U.S. Dist. LEXIS 104982 at *26 (citations omitted); *see also FTC v. Am. Standard Credit Sys., Inc.*, 874 F. Supp. 1080, 1089 (C.D. Cal. 1994) ("Authority to control the

To obtain monetary relief against such an individual, the FTC must additionally show that the individual knew or should have known of the deceptive practices.[155] The knowledge element does not require proof of the individual's subjective intent to defraud consumers; the individual need only have actual knowledge of material misrepresentations, reckless indifference to the truth or falsity of such representations, or an awareness of a high probability of fraud coupled with the intentional avoidance of the truth.[156] "Participation in corporate affairs is probative of knowledge."[157]

Defendant Martinos is the President and CEO of Elite.[158] From the beginning, Martinos has knowingly participated in the tech support scam. His name and signature appear on numerous corporate records.[159] He works directly with Elite's payment processors and responds to chargeback complaints.[160] Martinos testified during an administrative court hearing that he was intimately involved with and in charge of Elite's marketing practices.[161] According to a former employee, Martinos, among other Elite managers:

> "would repeatedly stress the importance of upselling customers cleanings and technical support services, and doing so by whatever means—typically by impressing upon customers that their computers were infected with viruses and that their personal information was at risk if they did not purchase Elite IT's services."[162]

Although "scamming was a common topic of discussion among employees[,]" Elite managers would tell employees who raised concerns that "the company is helping people clean their

---

company can be evidenced by active involvement in business affairs and the making of corporate policy"); *FTC v. Neovi, Inc.*, 598 F. Supp. 2d 1104, 1117 (S.D. Cal. 2008) (opining that the "authority to sign documents on behalf of the corporate defendant" can prove authority to control).
[155] *Freecom*, 401 F.3d at 1202-03; *LoanPointe*, 2011 U.S. Dist. LEXIS 104982 at *26-27.
[156] *Freecom*, 401 F.3d at 1207; *LoanPointe*, 2011 U.S. Dist. LEXIS 104982 at *26-27.
[157] *Id*. at *27.
[158] PX 19, pp. 587, 613, 843.
[159] PX 18, pp. 407, 420, 423, 451; PX 28, p. 1151.
[160] PX 28, pp. 1151, 1165-1178.
[161] PX 19, pp. 843-845, 849, 857-858.
[162] PX 13 ¶ 33.

computers and stay safe online."[163] According to former employees, Elite is primarily a family operation—with Martinos at the helm and present in the office, supported by his wife, Tracey, and two children, Heather and Jacob Martinos.[164]

C. An *Ex Parte* TRO With Additional Equitable Relief is Appropriate and Necessary.

The evidence demonstrates that the FTC is likely to succeed in proving Defendants are engaging in deceptive practices in violation of the FTC Act, the TSR, and ROSCA, and that the balance of equities strongly favors the public interest. Accordingly, preliminary injunctive relief is warranted. In order to stop Defendants' unlawful activities and to preserve the Court's ability to grant the final relief sought, the Court should enter an *ex parte* TRO that: (1) prohibits Defendants from engaging in conduct that violates the FTC Act, the TSR and ROSCA; (2) freezes Defendants' assets; (3) appoints a temporary receiver over Elite; and (4) grants the FTC and the temporary receiver immediate access to Elite's business premises and authorizes limited expedited discovery. As explained below, the ancillary relief requested through the Proposed TRO is necessary to protect consumers and to preserve the Court's ability to grant complete and permanent relief in this case.

1. The Court Should Stop the Defendants' Ongoing Scam.

Sworn consumer declarations, undercover calls, consumer complaints, and business and bank records show that Defendants are currently operating this tech support scam. To prevent ongoing consumer injury, the Court should enter a TRO that immediately prohibits Defendants from engaging in any conduct that violates the FTC Act, the TSR, or ROSCA, including making

[163] PX 15, p. 124.
[164] PX 13 ¶¶ 29-33 (former employee statement); PX 18, pp. 401-402 (bank records showing Tracey Martinos as signatory on Elite's account); PX 28, pp. 1176-1179 (emails showing Jacob Martinos interacting with ProPay on behalf of Elite).

misrepresentations concerning the identification of computer problems on consumers' computers.

According to Martinos, and as reflected in Elite's bank records, Elite also services business-to-business clients with IT support.[165] The records indicate this is approximately 7% of Elite's total revenue.[166] Since the FTC does not have any evidence indicating this line of business follows the fraudulent business model described in detail above, the TRO carves out this line of business by defining Tech Support Products and Services as those services marketed under Elite's dba Elite IT Home.[167]

As discussed above, this Court has broad equitable authority under Section 13(b) of the FTC Act to grant ancillary relief necessary to accomplish complete justice.[168] Because Defendants have continued their unlawful business practices unabated despite having notice of consumer complaints, former employee complaints, a cease and desist letter from Oath, termination from Microsoft's Network Partner program, and a payment processor shutting them down for excessive credit card chargebacks, immediate injunctive relief is necessary to protect additional consumers from being harmed by Defendants' ongoing unlawful practices.

2. The Court Should Freeze Defendants' Assets to Preserve the Possibility of Providing Redress to Defendants' Victims.

Bank records show that Defendants have received at least $10.7 million in proceeds from this tech support scheme.[169] These records also show that Defendants use their proceeds to

---

[165] PX 19, p. 844, PX 28, p. 1227.
[166] PX 24 ¶ 12, 14; PX 25 ¶¶ 5-10.
[167] Elite IT Home is the name Elite uses in emails consumers receive after purchase, and is the name of Elite's website that services consumers. *See, e.g.*, PX 19, pp. 628, 870.
[168] *F.T.C. v, Amy Travel*, 875 F.2d 875, 571-72 (7th Cir. 1989); *FTC v. H.N. Singer, Inc.*, 668 F.2d 1107, 1113 (9th Cir. 1982). *See also FTC v. Five-Star Auto Club*, 97 F. Supp. 2d 502, 532-39 (S.D.N.Y. 2000).
[169] PX 24 ¶ 14.

continue to pay attorneys' fees accrued in its litigation with Utah's Division of Consumer Protection over Defendants' failure to register as a telemarketer and continued telemarketing.[170] The Proposed TRO includes provisions that would freeze Defendants' assets and require them to provide financial disclosures. An asset freeze is necessary to preserve the status quo, ensure that funds do not disappear during the course of this action, and preserve the remaining assets for consumer redress and disgorgement.

In order to obtain an asset freeze, the FTC must show that it is likely to prevail on the merits.[171] In addition, some courts consider the conduct at issue. Where a company's business operations are permeated by fraud, as they are here, courts have found a strong likelihood that assets may be dissipated during the pendency of the case.[172] Others consider whether the amount of frozen assets will be sufficient to compensate consumers.[173] Here, an asset freeze is needed to preserve the Court's ability to provide restitution to victims. Bank records indicate that the amount of consumer injury far exceeds the amount of funds available for consumer redress.

---

[170] Legal fees and expenses constitute a dissipation of assets because these costs deplete the assets available for consumer redress. *FTC v. Triangle Media Corp.*, No. 18-cv-1388-MMA, 2018 U.S. Dist. LEXIS 144599, *22 (S.D. Cal. Aug. 24, 2018); *see also SEC v. Lottonet Operating Corp.*, No. 17-21033, 2017 U.S. Dist. LEXIS 51390, *55 (S.D. Fla. Mar. 31, 2017) (court found that dissipation of assets could include paying for legal fees).

[171] "[A]n injunction that maintains the status quo, such as an asset freeze, can be issued upon a 'showing that the probability of [the SEC] prevailing [on the merits] is better than fifty percent.'" *SEC v. Traffic Monsoon, LLC*, 245 F. Supp.3d 1275, 1296 (D. Utah 2017), *aff'd* 2019 WL 302867 (10th Cir.) (citing *SEC v. Cavanagh*, 155 F.3d 129, 132 (2d Cir. 1998)). Moreover, the court stated, "to the extent that the SEC seeks an asset freeze, proof of likelihood of future violations is not required." *Id*.

[172] *See, e.g., SEC v. Manor Nursing Centers, Inc.*, 458 F.2d 1082, 1106 (2d Cir. 1972) ("Because of the fraudulent nature of appellants' violations, the court could not be assured that appellants would not waste their assets prior to refunding public investors' money").

[173] *See, e.g., FTC v. IAB Mktg. Assocs., LP*, 972 F. Supp. 2d 1307, 1313, n.3 (S.D. Fla. 2013) ("there does not need to be evidence that assets will likely be dissipated in order to impose an asset freeze. The asset freeze is justified as a means of preserving funds for the equitable remedy of disgorgement"); *FTC v. World Patent Mktg., Inc.*, No. 17-CV-20848, 2017 WL 3508639, at *17 (S.D. Fla. Aug. 16, 2017) ("Dissipation does not necessarily mean that assets will be spirited away in secret; rather, it means that less money will be available for consumer redress").

Moreover, the FTC's experience in prior cases reveals that numerous defendants in other cases who were engaging in similarly serious unlawful practices have dissipated assets upon learning of an impending law enforcement action.[174] Under these circumstances, the risk of dissipation is high, and a temporary asset freeze is therefore necessary to preserve the Court's ability to award consumer redress. Such TRO provisions have been ordered in appropriate FTC cases.

3. The Court Should Appoint a Temporary Receiver Over Elite.

The Court should also appoint a temporary receiver over Elite pursuant to the Court's equitable powers under Section 13(b) of the FTC Act.[175] Appointment of a temporary receiver is appropriate where, as here, there is "imminent danger of property being lost, injured, diminished in value or squandered, and where legal remedies are inadequate."[176] When a corporate defendant has used deception to obtain money from consumers, "it is likely that, in the absence of the appointment of a receiver to maintain the status quo, the corporate assets will be subject to diversion and waste" to the detriment of victims.[177]

Appointment of a temporary receiver is particularly appropriate here because Elite's deceptive acts and practices demonstrate that Elite is likely to frustrate the FTC's law enforcement efforts by destroying evidence and/or dissipating assets. A temporary receiver will help prevent Elite from disposing of ill-gotten funds by identifying, securing, and controlling the use of Elite's assets, as well as marshaling and preserving its records. A temporary receiver will also assist in determining the full extent of the fraud and identifying additional victims of Elite's

---

[174] *See* Rule 65(b)(1) Certification of Federal Trade Commission Counsel Amanda R. Grier in Support of Ex Parte Motion For A TRO and Motion To Temporarily Seal Docket and Entire File, filed herewith.
[175] *U.S. Oil & Gas*, 748 F.2d at 1432.
[176] *Leone Indus. v. Assoc. Packaging, Inc.*, 795 F. Supp. 117, 120 (D.N.J. 1992).
[177] *First Fin. Group of TPX*, 645 F.2d at 438; *SEC v. Keller Corp.*, 323 F.2d 397, 403 (7th Cir. 1963).

scheme, as well as identifying any parts of the business that may be legitimate.[178] For these reasons, the Court should appoint a temporary receiver over Elite.

4. The Court Should Grant Expedited Discovery and Immediate Access to Elite's Business Premises.

In order to locate documents and assets related to the Defendants' scam, the TRO should authorize the FTC to engage in expedited discovery and allow the FTC and the temporary receiver immediate access to the Corporate Defendant's business premises and records. This relief is critical to the FTC's, the temporary receiver's, and the Court's ability to understand fully: (a) the scope of Defendants' business operations, their financial status, the participants involved, and their roles in the scheme; (b) the full range and extent of the Defendants' law violations; (c) the identities of injured consumers; (d) the total amount of consumer injury; and (e) the nature, extent, and location of the Defendants' assets.

Moreover, this relief is also necessary to protect against evidence destruction. As explained more fully in the Rule 65(b) Certification of Counsel Amanda R. Grier ("Grier Certification"), in the FTC's experience, it is likely that Defendants will take steps to destroy documents that relate to their scams. The proposed order includes provisions designed to grant access to Defendants' documents before they can be destroyed.[179] Courts in this District have granted *ex parte* TROs that include these provisions.[180] Accordingly, the Court should enter a TRO granting the FTC and the receiver immediate access and authorizing limited expedited discovery.

---

[178] As explained above, Defendants have a business-to-business line that makes up approximately 7% of its revenue. PX 24 ¶ 12, 14; PX 25 ¶¶ 5-10.
[179] District courts have broad and flexible authority in equity to depart from routine discovery procedures and applicable time frames, particularly in cases involving the public interest. *See* Fed. R. Civ. P. 26(d), 33(a), 34(b); *Porter v. Warner Holding Co.*, 328 U.S. 395, 398 (1946).
[180] *See supra* note 129.

5. The Court Should Issue the TRO *Ex Parte*.

An *ex parte* TRO is necessary because, if provided with advance notice,[181] Defendants are likely to dissipate and conceal assets and destroy evidence. Defendants have disregarded court orders and calls from industry and consumers to cease their conduct, and they have continued their fraudulent activity despite their payment processor shutting them down for high credit card chargeback rates.[182] Given these facts, and the fraudulent nature of their business, there is a significant likelihood that they would also disregard the Court's TRO or evade its provisions, including those related to the preservation of assets and records. This would defeat the purpose of a TRO.[183]

Records also show Defendants' apparent willingness to misrepresent or mislead in order to avoid accountability for their business practices. Throughout the administrative process with the Utah DCP, Defendants have argued that they are not telemarketers under the statute and should not have to register because it would harm their business.[184] Even after exhausting the process, including an administrative hearing with evidence and live testimony, and an ongoing enforcement action by the Utah Attorney General's Office, Defendants refuse to register as a telemarketer.[185]

---

[181] Fed. R. Civ. P. 65(b) authorizes the Court to issue a TRO *ex parte* if "immediate and irreparable injury, loss, or damage will result" from advance notice to Defendants. To further prevent premature notice, the FTC has filed concurrently an *Ex Parte* Motion to Temporarily Seal Entire File and Docket. In support of the FTC's requests for an *ex parte* TRO and to temporarily seal this case, FTC counsel has filed concurrently a written Certification.

[182] PX 19 ¶¶ 21-23; PX 15, pp. 133-136; PX 13 ¶ 24; PX 28, p. 1161.

[183] *See, e.g., FTC v. Int'l Computer Concepts, Inc.*, No. 5:94-CV-1678, 1994 WL 730144, at *16 (N.D. Ohio Oct. 24, 1994) ("Where, as in this case, business operations are permeated by fraud, there is a strong likelihood that assets may be dissipated during the pendency of the legal proceedings…. Without an immediate freeze of assets, it is unlikely that funds will be available to satisfy any final order….") (internal citation omitted).

[184] PX 19 ¶¶ 4, 6, pp. 856-857.

[185] PX 19 ¶¶ 21-23. Martinos testified at the adminstrative hearing that he believes if he registers as a telemarketer, Google will blacklist his company and block his Google Adwords account for life, which will wipe out the company. *Id*. at 856-57.

In Defendants' response to Oath's Cease and Desist letter, Defendants denied every allegation, including the allegation that Elite misrepresented to consumers its affiliation with Yahoo.[186] However, consumer complaints and former employee statements show otherwise.[187] In response to complaints from the Utah DCP, Utah BBB, and credit card chargeback documents from Propay, Defendants routinely state that consumers authorized the charges and are fully aware of the transaction. However, Defendants fail to state that consumers are lied to about the state of their computers in order to induce them to make the purchase and they fail to tell consumers prior to purchase that there are no refunds, there is a $150 cancellation fee, and the preventative maintenance package is a negative option plan that automatically renews.

Finally, Defendants demonstrated their willingness to knowingly conceal and misrepresent the true nature of Elite's business when Martinos misrepresented Elite's business in order to avoid the scrutiny that acquiring banks give to tech support companies like Elite.[188] Martinos first asked its existing payment processor to change Elite's merchant category code to one that would garner less scrutiny and keep its merchant account open. When his attempt failed, Martinos used an incorrect merchant account code in Elite's application to obtain a merchant account with a different processor.

The evidence establishes that there is a strong likelihood that Defendants would conceal or dissipate assets absent *ex parte* relief. As such, it is in the interest of justice to provide the requested *ex parte* relief to prevent the dissipation of assets or the destruction of evidence, which will maintain the status quo and preserve this Court's ability to award full and effective final relief.

[186] PX 15, pp. 133-36.
[187] PX 13 ¶ 20; PX 15, pp. 120-124, 127-128, 131; PX 27, p. 1039.
[188] *See* Section II.A.11.

IV. CONCLUSION

Given the compelling evidence showing the insidious and pervasive nature of Defendants' tech support scam, the FTC respectfully moves the Court *ex parte* for a TRO that will protect consumers, prevent further harm, and preserve the Court's ability to provide complete and permanent relief to the injured. The FTC has proposed a TRO that will immediately halt Defendants' scam, freeze Defendants' assets, appoint a temporary receiver, and provide immediate access to Defendants' business premises in order to preserve assets and documents for consumer redress. The FTC also requests that the Court order Defendants to show cause why a preliminary injunction should not issue against them.

Respectfully submitted,

Dated: February 25, 2019

Amanda Grier
Colleen B. Robbins
Elsie B. Kappler
Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-3845; agrier@ftc.gov
(202) 326-2548; crobbins@ftc.gov
(202) 326-2466; ekappler@ftc.gov
Attorneys for Plaintiff
FEDERAL TRADE COMMISSION